REMARKS

The examiner rejected Claims 1-12 and 15-33 under 35 U.S.C. 102(e) as being anticipated by Yavatkar et al., (Yavatkar) U.S. Patent No. 6,735,702.

The Examiner stated:

> **As to claim 1, Yavatkar teaches a method of protecting a data center against a denial of service attack, the method comprises:**
> **sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, that sample network packets and collect statistical information on network packets sent over the network, to request the statistical information from at least some of the data collectors, the statistical information to determine the source of suspicious network traffic heir sent to the data center (col. 3, lines 25-37 and col. 18, lines 32-53, agents are deployed at different areas of the network for the detection and diagnosing of various network attacks as well as for collecting statistical information on a particular node).**

Applicant's claim 1 is distinct over Yavatkar et al, since the reference fails to suggest ... sending queries to data collectors, deployed at different points in a network that carries network traffic to the data center, the data collectors collect statistical information on network packets sent over the network, the queries to request the statistical information from at least some of the data collectors and processing the statistical information to determine the source of suspicious network traffic sent to the data center.

Yavatkar discusses at Col. 3, lines 25-37:

> **The system and method of an exemplary embodiment of the present invention use agents--mobile software modules--to collect data on the state of a network during a network attack, allowing for more accurate diagnosis of an attack. During a network attack, the system and method of the present invention allow for details on the attack traffic (e.g., the source of the attack traffic and path of the attack traffic) to be gathered. The source of the attack traffic may be the originator of the attack traffic or, for example a gateway allowing attack traffic to enter a network and which is, in effect, the source of attack traffic to the network. Such information then may be used to halt the attack or insulate the network from the attack.**

and at col. 18, lines 32-53:

To report, the bloodhound agent moves across the network to the node of its launch point and provides its findings to the watchdog agent. The bloodhound agent transmits the data it has collected to the watchdog agent using a messaging service. After reporting, the bloodhound agent is destroyed. In an exemplary embodiment, the bloodhound agent provides to the watchdog agent a report indicating the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic. The source may be indicated as a gateway allowing access to other networks; in such a case the indicated source is not the originating source of the attack. The path as described by the bloodhound agent comprises links and nodes. Links may be denoted using pairs of port/node combinations. For example, a link may be denoted as the link connecting port "Interface 2" on node 22.49.1.3 to port "Interface 4" on node 22.49.1.7. In alternate embodiments the findings may include other types of information. In an alternate embodiment the bloodhound agent need not move to its launch point to report its findings; for example, it may transmit the information across the network using a messaging service and then self-destruct.

The examiner equates the data collectors to the bloodhound agents described by Yavatkar ("agents are deployed at different areas of the network for the detection and diagnosing of various network attacks as well as for collecting statistical information on a particular node" Office action page 3). While the bloodhound agents provide findings to the watchdog agent, and transmit a report it has collected, Yavatkar describes a report indicating "the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic." Yavatkar also describes: "The path as described by the bloodhound agent comprises links and nodes. Links may be denoted using pairs of port/node combinations." However, Yavatkar also describes that the bloodhound agents "self destruct."

There is no suggestion in Yavatkar that the bloodhound agents are responsive to queries for statistical information. Indeed statistical information on network traffic is neither described nor suggested by Yavatkar. Rather, Yavatkar is directed to a process in which the bloodhound agents travel from node to node in an attempt to provide a path of an attack.

Yavatkar also mentions that: "In alternate embodiments the findings may include other types of information." However, as Yavatkar describes the bloodhound agents, the bloodhound agents sample traffic "to search for the attack traffic."

In step 406 bloodhound agent 116, in the hunting mode, analyzes traffic being received at the node on which it currently executes (its "current node") to identify the port receiving the most attack traffic. Bloodhound agent 116 analyzes traffic according to the type of attack traffic for which it is configured. The initial current node may be the node of the bloodhound agent's launch point, or may be a

> **different node. Bloodhound agent 116 samples packets received by and/or sent by the various ports of the current node to search for attack traffic. Bloodhound agent 116 uses its work object and worksheet to use services to access ports on the current node, ignoring ports connected to links it already analyzed.**

Yavatkar neither describes nor suggests a technique in which statistical information on network traffic is collected, sent from the data collectors in response to the queries, and processed to determine the source of suspicious network traffic sent to the data center.

Claim 1 processes statistical information pertaining to such traffic, which is often spoofed, to pinpoint and identify the source of the attack.

Yavatkar also teaches away from querying the agents. In the Background, Yavatkar describes:

> **A similar analysis may be performed from a central console which may query remote nodes for information about the source of incoming traffic. Such a diagnosis is also slow and inaccurate, as it requires commands to nodes and responses from nodes to be transmitted across the network. The speed at which attacks occur and the speed at which such problems must be fixed makes such detection methods ineffective. A path taken by traffic may be described as the equipment traversed by traffic as the traffic crosses a network or networks (e.g., a series of nodes and links, or a series of sub-networks).**

Claim 1 further includes the feature of: "sending the statistical information from the data collectors in response to the queries for processing the statistical information to determine the source of suspicious network traffic sent to the data center." In contrast, Yavatkar teaches to process reports "indicating the path or paths (or a portion of the path or paths) taken by the attack traffic." Thus, claim 1 is allowable over Yavatkar since the references neither describes nor suggest all of the features of claim 1.

Claims 2-14 are directly or indirectly dependent on claim 1 and are allowable at least for the reasons discussed in claim 1, and further add distinct limitations.

For example, Claim 2 adds the feature of sending queries to the data collectors for the statistical information based on victim destination address.

The examiner contends these features are disclosed in Yavatkar, at (col. 13, lines 44-53 and col. 3, line 65 - col. 4, line 23. These passages from Yavatkar are reproduced below:

> **In an exemplary embodiment of the present invention, a watchdog agent monitors the node on which it operates for traffic having characteristics of a network attack. A watchdog agent may also monitor for and detect a network attack at a device other than the device on which it operates. On detecting an attack the watchdog agent launches one or more bloodhound agents to trace the attack traffic. The watchdog agent launches various types of bloodhound agents based on the type of attack detected; each bloodhound agent is designed to trace traffic from one type of attack. In an exemplary embodiment a bloodhound agent moves across the network, tracing the path or paths taken by attack traffic. To trace attack traffic, the bloodhound agent follows an iterative process of finding the port for the link on the node on which it operates which is accepting attack traffic, attempting to traverse that link (i.e., to move to the node on the other side of the link) to a new node, and, once at the new node, again finding the port and link which are accepting attack traffic. In such a manner the path or paths, or a portion of the path or paths, of attack traffic between the source of the attack traffic and the target node may be found. After gathering such information a bloodhound agent reports to the watchdog agent, which, in turn, may report to a human operator or, possibly, attempt to halt the attack. A target node is a node to which attack traffic is directed or which attack traffic affects. [Yavatkar, col. 13, lines 44-53].**
>
> **If the source of the attack traffic messages can be identified (by, for example, its IP address) the source can be shut down or disabled. For example, the Internet provider allowing the source device access to the Internet may be notified and may terminate the source device's Internet access. However, through the use of IP spoofing the source of the attack may be obscured. Using IP spoofing the TCP/IP packets constituting the attack traffic indicate a source which is not the actual source device--the sender of the attack traffic inserts a false "return address." [Yavatkar, col. 3, line 65 - col. 4, line 23].**

One or ordinary skill in the art would not recognize from these passages or elsewhere in Yavatkar, the features of claim 2. It is clear from the above that Yavatkar does not describe or suggest that statistical information based on victim destination address is sent from the data collectors or that Yavatkar suggests sending queries to the data collectors. Yavatkar discloses that the bloodhound agents report to the watchdog agents, which may report to a human operator. However, the report is of the path taken by the attack, not statistical information, and further the Yavatkar does not suggest that the report is sent in response to a query from the watchdog agent. Rather, the report appears to be send prior to the bloodhound agent self-destructing.

Claim 6 distinguishes by reciting that the queries and the statistical information are sent over a redundant network that does not carry the packet traffic .... .

The examiner contends that the feature previously recited "hardened network" was disclosed in Fig. 2. However, no such feature is shown in Fig. 2. Nonetheless, Applicant has amended claim 6 to recite that the queries and the statistical information are sent over a

redundant network that does not carry the packet traffic. Neither Fig. 2 in Yavatkar nor elsewhere is this feature disclosed.

Claim 11 serves to further limit claim 1 by reciting that if a source of the attack is not behind a gateway, the control center queries the data collectors to provide information about possible locations of the attacking system. As was discussed above, Yavatkar does not teach that the bloodhound agents are queried by the watchdog agents and further teaches away from this feature.

Claim 15 is distinct over Yavatkar. Claim 15 recites the features of a method of protecting a victim data center against a denial of service attack. Claim 15 includes ... receiving, from a gateway ... a notification that the victim data center is under an attack, sending queries to data collectors deployed at different points in a network that carries network traffic ... the queries being requests for statistical information from data collectors that have examined network traffic with the victim destination address and determining the data center or centers involved in the attack on the victim data center by analyzing collected statistical information from the data collectors.

The examiner contends that Yavatkar teaches sending queries and determining at (col. 3, lines 25-37 and col. 18, lines 32-53). Applicant disagrees. At col. 3 Yavatkar merely discusses spoofed attacks, but does not suggest either of these features. At. Col. 18 Yavatkar merely discusses that the bloodhound agent reports to the watchdog agent and then after reporting is destroyed. Yavatkar does not suggest that the bloodhound agent is responsive to a query from the watchdog agent, nor that any querying of the bloodhound agent would be feasible. This would follow, because the bloodhound agent has a self triggered reporting mechanism that goes into action after it is finished and just before it is destroyed. See 422 and 424 of Fig. 9, for example.

Claim 16 further distinguishes by reciting communicating statistical information from the control center to/from a gateway device that is disposed with the victim data center. Yavatkar does not communicate any statistical information and hence does not communicate such information to/from a gateway.

Claim 20 is directed to a system to thwart denial of service attacks on a victim data center. Claim 20 is allowable over Yavatkar since the reference fails to suggest a plurality of monitors ... collecting statistical data on network traffic, a control center to ... send queries to data collectors to request the statistical information from data collectors, the statistical information used to determine the source of suspicious network traffic being sent to the victim. Claim 20 also includes the feature of a gateway device ...disposed to protect the victim data center, and being coupled to the control center.

This combination of features is not suggested by Yavatkar. Yavatkar fails to suggest the plurality of monitors collecting statistical information, or sending queries from the control center to the monitors for the statistical information in response to receiving the notification of an attack. Yavatkar does not teach querying in response, but rather teaches to launch the bloodhounds,

Claim 21, which recites that the data collectors collect statistical information on network packets that pass through points in the network that the data collectors monitor, is not suggested for reasons that now should be apparent to the examiner.

Claim 22 distinguishes by reciting that the control center ... determines a source of the attack on the victim data center by analyzing collected statistical information from the data collectors. In Yavatkar, the watchdog agent receives the path of the attack from the non destroyed bloodhound agents, not statistical information that is analyzed to determine the source.

Claim 23 distinguishes since Yavatkar fails to suggest that the control center and gateway device associated with the victim data center exchange data including statistical information to thwart the attack.

Claim 24 distinguishes since Yavatkar fails to suggest that data between the control center and gateway device associated with the victim data center are sent over a redundant network that is a different network than the network that is being monitored by the data collectors, as discussed above.

Claims 25-28 add additional distinguishing features. Claim 29 and claims 30-33 are allowable for analogous reasons as in claims 20-28.

Enclosed is a **$60** check for the Petition for Extension of Time fee. Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 3/9/06

Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906

21257781.doc